Request for Information
Cyber Supply Chain Risk Management

1. **Brief Description of Information Sought.**

This Request for Information (RFI) is being issued to assist the Government in market research about industry capabilities to provide information and communications technology (ICT) supply chain risk information through provision of “due diligence” research based on publicly and commercially available unclassified data. DHS seeks information about capabilities that address risk as a function of threat, vulnerability, likelihood, and consequences, and aggregate multiple data sets into structured archives suitable for analysis and visualization of the relationships of businesses, individuals, addresses, supply chains, and related information.

The information generated through the due diligence capability will be shared between organizations and may be used in combination with other information to broadly address supply chain risks to Federal, State, Local, Tribal, and Territorial governments, and Critical Infrastructure owners and operators (hereinafter, “stakeholders”).

The government seeks information about capabilities that enable identification and mitigation of ICT products (e.g., hardware, software, devices) that may contain potentially malicious functionality, are counterfeit, are vulnerable due to deficient manufacturing practices within the supply chain, or are otherwise determined to enable or constitute a threat to the United States.

The government also seeks information about capabilities that enable identification and mitigation of supply chain risks presented by ICT-based services (e.g., cloud services, managed services), as well as service providers that use ICT and the ICT contains, transmits, or processes information provided by or generated for the stakeholder to support the operations or assets of a stakeholder entity (e.g., professional services).

The categories of capability offerings that the government is interested in learning more about include (1) supply chain risk due diligence information; and (2) tool, product or system solution used to deliver due diligence information.

2. **Background.**

This RFI is intended to build upon the knowledge gained from prior information requests and industry and stakeholder engagements related to business due diligence and supply chain risk management.

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. It covers the entire lifecycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an ICT product or service at any stage of the lifecycle.

Request for Information
Cyber Supply Chain Risk Management

The Department of Homeland Security (DHS), all other Federal, State, Local, Tribal, and Territorial governments, and Critical Infrastructure owners and operators are highly dependent on vendors and integrators of ICT (including IoT) to accomplish their various missions, and as a result, the global ICT supply chain is a significant source of risk to the nation.

The government anticipates due diligence research will be conducted on selected suppliers that provide products, services, or solutions which connect in any way to a stakeholder information system or which contain, transmit, or process information provided by or generated for the stakeholder to support the operations and assets of a stakeholder entity. Possible subjects of due diligence research include all companies directly involved in delivery of products, services, and solutions to stakeholders, through all tiers of the supply chain.

Examples of how due diligence information may be shared with stakeholders include, but are not limited to:

- Shared without enrichment; and
- Shared after enrichment with government or other stakeholder data.

Examples of how due diligence information may be used by stakeholders include, but are not limited to:

- Assisting in market research, development of source selection evaluation criteria and other solicitation provisions, and contract performance indicators;
- Supporting testing and evaluation activities and information system authorizations;
- Measuring contractor performance; and
- Supporting more detailed supply chain risk assessments, audits, or investigations.

3. **Intended purpose.** The DHS intends to use the information received in response to this RFI for planning purposes and to help define requirements for a cyber supply chain risk assessment capability to support stakeholders.

    3.1. Objectives for this capability include:

        3.1.1. Affordable;
        3.1.2. Automated process supported by threat analysis;
        3.1.3. Scalable, and Extensible - to facilitate growth and ability to add capability;
        3.1.4. Promote consistency and a common approach(e.g. taxonomy, standards and processes);
        3.1.5. Enable information-sharing;
        3.1.6. Minimize duplication of effort and cost from better decision-making, using a shared solution, centralized purchase of data sets, and reuse of due diligence information; and
        3.1.7. Aligned, as much as possible, with similar practices, such as those emerging or evolving in the vendor community and insurance industry

3.2. No proposals are being requested or accepted with this notice. No contract shall be awarded from this notice. This special notice does not constitute a request for a quote or proposal for the procurement of products or services.

3.3. In order to obtain additional information, the Government may hold an industry day or schedule one-on-one meetings.

4. **Submission Requirements.** Submissions must be:

4.1. Received no later than 5:00 pm Eastern Daylight Time Wednesday, October 10, 2018.

4.2. Sent via email in Adobe (.pdf) or Microsoft Word (.docx) format to: Contract Specialist, Christiane Lynch at Christiane.Lynch@hq.dhs.gov and Contracting Officer, Paula Nusbaum at Paula.Nusbaum@hq.dhs.gov.

4.3. Twelve (12) pages or less in length, 12 point font, with 1 inch margins

4.4. Unclassified and appropriately marked if containing proprietary information

5. **Statement of Limitations.**

5.1. The Government represents that this RFI, submissions from respondents to this RFI, and any relationship between the Government and respondents arising from or connected or related to this RFI, are subject to the specific limitations and representations expressed below, as well as the terms contained elsewhere in this RFI. By responding to this RFI, respondents are deemed to accept and agree to this Statement of Limitations. Respondents to this RFI acknowledge and accept the Government's rights as set forth in the RFI, including this Statement of Limitations.

5.2. The Government reserves the right, in its sole discretion, without liability, to use any or all of the RFI responses in its planning efforts. The Government reserves the right to retain and use all the materials, information, ideas, and suggestions submitted in response to this RFI.

5.3. This RFI shall not be construed in any manner to implement any of the actions contemplated herein, nor to serve as the basis for any claim whatsoever for reimbursement of costs for efforts expended in preparing a response to the RFI.

5.4. The submission of an RFI response is not required to participate in any potential future development process or RFP.

5.5. To the best of the Government's knowledge, the information provided herein is accurate. Respondents should undertake appropriate investigation in preparation of responses.

5.6. This RFI is issued solely for information and planning purposes and does not constitute a solicitation. Responses to this notice are not an offer and cannot be accepted by the Government to form a binding contract.

5.7. The Government will not enter into any exchange, sale, lease, or other agreement as a result of this RFI. The Government will not reimburse RFI respondents for any expenses associated with responding to this RFI, though the Government sincerely appreciates respondents' efforts and input. The Government may, at some point in the future, issue a Request for Proposals (RFP).

5.8. The Government intends to use the information received in response to this RFI for planning purposes and to help make strategic decisions regarding establishing a business due diligence/cyber supply chain risk assessment program capability that is anticipated and will need to scale to be able to support multiple agencies or function as a government-wide shared service.

5.9. Questions regarding this RFI may be submitted via e-mail to Contract Specialist, Christiane Lynch at Christiane.Lynch@hq.dhs.gov and Contracting Officer, Paula Nusbaum at Paula.Nusbaum@hq.dhs.gov.

6. Request for Information – Questions for Respondents

6.1. Company Information

6.1.1. Provide a brief introduction/description of your company, business size, and the PRIMARY North American Industry Classification System (NAICS) code that your company uses.

6.1.2. If your company is a small business, please indicate your firm's socioeconomic status (i.e. inclusion under 8(a) Small business, Small Disadvantaged business, Women Owned Small business, SDVOSB, HUBZONE, or other socioeconomic business program.

6.2. Due Diligence Information Capability

6.2.1. Do you currently offer a due diligence capability? If yes, describe, including what types of information the capability includes (e.g., financial, cybersecurity, physical security, personnel, legal, etc.).

6.2.2. Is your offering cloud-based? If yes, do you have a current FedRAMP authorization?

6.2.3. Describe how you establish confidence in the veracity of the source(s) of the data used to develop due diligence information.

6.2.4. Does the capability include information about any of following subjects? If yes, describe.

6.2.4.1. Provenance (chain-of-custody)

6.2.4.2. Trade Agreements Act Compliance

6.2.4.3. Component Bill of Materials

6.2.4.4. Testing and Evaluation
6.2.4.5. Marking/Labeling
6.2.4.6. Product or Component Vulnerability(ies)
6.2.4.7. Other (Describe)

6.2.5. Describe manual processes vs. automated processes associated with your offering.

6.2.6. If your offering is delivered via software or software-as-a-service, describe configurability options and constraints.

6.2.7. If your offering is delivered via software or software-as-a-service, describe interoperability options and constraints.

6.2.8. Describe how due diligence information is delivered to the user.

6.2.9. Describe any options or constraints with regard to accessing, aggregating, storing, reusing, or retaining due diligence information by the government.

6.2.10. Indicate which of the following functions/capabilities are included in your offering. For each one that is included, identify whether this capability is included as part of the "core" offering, is available as an additional option, or is available via a third party partner or sub-tier supplier with whom you have an existing relationship.

6.2.10.1. Self-service features
6.2.10.2. Search
6.2.10.3. APIs
6.2.10.4. User-Controlled Data or Files Import/Export
6.2.10.5. Database
6.2.10.6. Data Aggregation
6.2.10.7. Risk Scoring
6.2.10.8. Dashboard
6.2.10.9. Analytics
6.2.10.10. Network Mapping
6.2.10.11. Other Visualizations (Describe)
6.2.10.12. Alerts
6.2.10.13. Automated Report Creation
6.2.10.14. Automated Workflow
6.2.10.15. Continuous monitoring and updating
6.2.10.16. Archives - Access to Historic Data/Information
6.2.10.17. Other (Describe)

6.3. Implementation and Ongoing Operations and Maintenance

6.3.1. Provide a brief description of the approach the firm would take in providing the capability contemplated in this RFI or a recommendation of the approach the government should take in implementing the capability.

6.3.2. Briefly describe the activities that need to occur during the implementation phase (Purchase/Award to "Go-Live"/Initial Use).

6.3.3. Will the Government have any ongoing responsibilities for operations and maintenance of the due diligence tool/product/solution? If yes, briefly describe.

6.4. **Scalability and Extensibility.** The Government would like to understand to what extent the current offering is scalable (e.g., to meet spikes in demand, accommodate increased in utilization rate or number of concurrent users) and "extensible" (e.g., able to be augmented with additional functionality).

6.4.1. Describe "scalability" current capabilities and constraints. Description should demonstrate the respondent's success in increasing volume of services provided without any deterioration in the quality of service.

6.4.2. Describe "extensibility" current capabilities and constraints. Description should demonstrate the respondent's success in increasing volume of services provided without any deterioration in the quality of service.

6.5. **Pricing.** Being able to realize "economies of scale," affordability to implement, and reasonableness and predictability of ongoing costs are key objectives for the Government.

6.5.1. Are there "cost line items" for your offering that can be priced out separately? For these cost line items, what is pricing based upon?

6.5.2. If applicable to your offering, please provide rough order of magnitude pricing information for due diligence information for each company researched. Are discounts available based upon volume or some other factor(s)?

6.5.3. If applicable to your offering, please provide rough order of magnitude pricing information for user licensing. Is "enterprise" licensing an option? Are discounts available based upon number of users or some other factor(s)?

6.5.4. Does your pricing depend on whether the information will be shared (with or without enrichment) between stakeholders?

6.5.5. Provide any additional comments you may have concerning the Government's pricing objectives.